**БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 1 (112).** – 74–89

*МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*

УДК 004 DOI: 10.17212/2782-2230-2024-1-74-89

# АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ХРАНЕНИЯ ПАРОЛЕЙ*

Д.К. РЯБЦЕВ

*630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: ryabtsev@mail.ru*

Настоящая статья представляет всесторонний обзор существующих подходов к безопасному хранению паролей в современных информационных системах. Исследование охватывает технологии, используемые для защиты учетных данных, и их эффективность в контексте растущих угроз в области кибербезопасности. Читатель получит глубокое понимание преимуществ и недостатков различных методов хранения паролей, а также рекомендации по выбору наиболее надежных и современных решений.

**Ключевые слова**: безопасность паролей, хеширование, соль в защите паролей, криптография, многофакторная аутентификация, биометрические технологии

## ВВЕДЕНИЕ

С ростом технологической зависимости общества и переходом к цифровой среде вопрос безопасности данных становится более актуальным, чем когда-либо. Одним из ключевых аспектов обеспечения информационной безопасности является правильное хранение учетных данных, в частности паролей пользователей. Стремительное развитие киберугроз и постоянные попытки несанкционированного доступа подчеркивают необходимость эффективных методов хранения паролей.

В настоящей статье проанализированы современные методы хранения паролей, начиная от классических хэш-функций до инновационных подходов, таких как многофакторная аутентификация и биометрические технологии. Рассмотрены их преимущества, недостатки, а также уровень защиты, который они предоставляют в условиях постоянно меняющегося киберпространства.

* Статья получена 15 февраля 2024 г.

# 1. ТРАДИЦИОНЫЕ МЕТОДЫ ХРАНЕНИЯ ПАРОЛЕЙ

## 1.1. ХРАНЕНИЕ ПАРОЛЕЙ В ВИДЕ ОТКРЫТОГО ТЕКСТА

Опасность хранения паролей в открытом тексте становится явной при рассмотрении современных требований к безопасности информации.

В контексте кибербезопасности, когда технологии постоянно совершенствуются, хранение паролей в открытом виде является не только ненадежным, но и крайне рискованным. В случае утечки базы данных злоумышленники могут мгновенно получить доступ ко всем аккаунтам пользователей, представляя серьезную угрозу как для физических лиц, так и для организаций. Примером может служить инцидент с социальной сетью MySpace, когда украденные учетные данные оказались доступными в открытом виде, что привело к компрометации миллионов аккаунтов.

Без криптографической защиты пароли оказываются подвержены различным атакам, включая атаки по методу подбора, перехвата трафика и атаки внутри самой системы. Это делает данный метод крайне уязвимым и несостоятельным в условиях современного цифрового ландшафта.

Однако кроме технических аспектов существуют и организационные проблемы, связанные с хранением паролей в открытом виде. Администрирование учетных данных становится гораздо сложнее, поскольку изменения в паролях требуют массовых обновлений, что может существенно снизить эффективность системы управления доступом. Также не стоит забывать об отсутствии гибкости в политиках безопасности: пароли в открытом виде ограничивают возможности установки сложных политик безопасности, таких как требование к длине пароля, использование символов и периодическая смена пароля.

## 1.2. ХЕШИРОВАНИЕ ПАРОЛЕЙ. ПРИМЕНЕНИЕ СОЛИ

Хеширование паролей считается надежным методом обеспечения безопасности учетных данных в современной кибербезопасности. Этот подход, который преобразует пользовательский пароль в уникальный хеш, играет ключевую роль в устойчивости систем к различным киберугрозам.

Криптографическая стойкость является фундаментальной характеристикой хеширования паролей, обеспечивает устойчивость к восстановлению и обратному расшифровыванию. Проблема коллизий, когда два набора вход-

ных данных могут привести к одному хешу, минимизируется с использованием криптографически стойких хеш-функций.

Дополнительные меры безопасности, такие как соль для уникальности и предотвращения использования заранее вычисленных таблиц и итерации для замедления процесса атак, существенно усиливают защиту паролей. Современные хеш-алгоритмы, такие как SHA-256 и bcrypt, предоставляют высокий уровень безопасности и широко применяются в кибербезопасности.

Хеширование паролей также играет важную роль в многофакторной аутентификации, где хеш пароля является одним из компонентов уникального идентификатора пользователя.

Хеширование паролей остается неотъемлемым элементом в борьбе с киберугрозами. Важно осознавать, что угрозы постоянно меняются, и использование дополнительных мер безопасности, таких как многофакторная аутентификация, становится всё более важным аспектом современных стратегий защиты.

## 1.3. ШИФРОВАНИЕ ПАРОЛЕЙ

Шифрование паролей представляет собой неотъемлемый элемент в обеспечении кибербезопасности, обеспечивая эффективный уровень защиты для учетных данных пользователей. Этот процесс преобразования паролей в непонятные для человека данные с использованием алгоритмов и ключей шифрования играет решающую роль в современных стратегиях безопасности.

Используемые алгоритмы, такие как AES, DES и RSA, поддерживают симметричное и асимметричное шифрование, предоставляя разные степени безопасности в зависимости от конкретных требований и контекста применения.

Шифрование паролей не только обеспечивает защиту от перехвата трафика, предотвращая прослушивание данных, но также является эффективным механизмом защиты от атак перебора.

Важную роль шифрование играет в безопасности хранения данных, особенно в контексте баз данных, где оно дополнительно обеспечивает защиту учетных записей при возможной утечке данных.

Методы шифрования также находят свое место в многофакторной аутентификации, где шифрованный ключ может быть одним из компонентов подтверждения личности пользователя.

Сложившийся тренд в современных исследованиях – это использование квантового шифрования, обещающего еще более высокий уровень безопасности в условиях постоянного развития вычислительных технологий.

Таким образом, эффективное использование шифрования паролей остается критически важным вопросом в стратегиях безопасности, помогая предотвращать угрозы в постоянно изменяющемся цифровом мире.

## 1.4. ХРАНЕНИЕ ПАРОЛЕЙ В БРАУЗЕРАХ. ОСОБЕННОСТИ И РИСКИ

Хранение паролей в браузерах становится неотъемлемой частью нашей цифровой жизни. Это удобство сопровождается рядом особенностей и рисков, которые требуют внимательного рассмотрения.

Браузеры предлагают автоматическое заполнение полей ввода, облегчая процесс входа на сайты. Также предоставляется синхронизация паролей между устройствами и инструменты для управления безопасностью, включая проверку на утечку данных.

Однако существуют риски. Безопасность хранилища под угрозой, и уязвимости в браузере могут привести к утечке учетных данных. Доступ к учетным данным возможен, если злоумышленник получит контроль над устройством пользователя. Синхронизация между устройствами может стать слабым местом без должной осторожности. В качестве примера следует привести результаты исследования из Университета Карнеги Меллон, в котором профессор Рауль Гонсалес смог доказать, что автозаполнение браузеров – одно из самых уязвимых мест, и оно не подходит для хранения паролей. Исследователи создали Lupine – инструмент сетевого уровня для кражи паролей, хранящихся в браузере жертвы. План имитации атаки выглядел следующим образом.

1. Злоумышленник ждет, пока жертва сделает запрос к незашифрованной странице, обслуживаемой по HTTP, а затем добавляет к ответу большое количество iframe, каждый из которых указывает на другую веб-страницу.

2. После того как браузер жертвы получит подделанный ответ, он впоследствии сделает запросы к веб-страницам, связанным с каждым iframe.

3. Злоумышленник снова перехватывает эти запросы и отвечает на каждый веб-запрос поддельной веб-страницей, содержащей форму входа и фрагмент кода.

4. Когда поддельные страницы доставляются в браузер жертвы, они заставляют менеджер паролей браузера автоматически заполнять пароли для страницы.

Результат исследований браузеров на безопасность функции автозаполнения показан в табл. 1.

Таблица 1

Table 1

**Исследование безопасности функции автозаполнения в браузерах**

**Investigating the security of autofill functionality in browsers**

| Браузеры | URL-требования | Требования к действиям пользователя | DOM-требования |
|---|---|---|---|
| Internet Explorer | Происхождение и путь исходного адреса должны совпадать | Необходимо ввести первый символ имени пользователя | Нет |
| Opera | Происхождение исходного адреса должно совпадать | Необходимо нажать на кнопку автозаполнения или нажать Control + Enter | Происхождение адреса назначения должно совпадать. Атрибут name полей ввода должен совпадать |
| Safari | Происхождение исходного адреса должно совпадать | нет | Форма входа должна находиться внутри рамки верхнего уровня |
| Firefox | Происхождение исходного адреса должно совпадать | нет | Происхождение адреса назначения должно совпадать |
| Chrome | Происхождение исходного адреса должно совпадать | нет | Происхождение адреса назначения должно совпадать |

Советы по безопасному использованию включают применение «мастер-пароля» для дополнительной защиты, регулярную проверку и обновление сохраненных паролей, а также отключение синхронизации для чувствительных аккаунтов. Хотя хранить пароли в браузерах удобно, важно поддерживать баланс между удобством и безопасностью, регулярно обновляя знания о кибербезопасности и следуя рекомендациям для защиты своих данных.

# 2. ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

## 2.1. ОПИСАНИЕ И ПРЕИМУЩЕСТВА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Двухфакторная аутентификация (2FA) становится неотъемлемым элементом современных стратегий кибербезопасности, предоставляя дополнительный уровень защиты учетных данных. Этот метод подтверждения личности пользователя включает два компонента, усиливая безопасность входа в системы и онлайн-аккаунты.

Преимущества двухфакторной аутентификации явно видны в контексте современных угроз кибербезопасности. Первым фактором обычно выступает последовательность, которую пользователь расценивает как пароль. Второй фактор представляет собой биометрические данные или одноразовый код. Основное преимущество 2FA заключается в том, что даже если злоумышленник узнает пароль, ему всё равно будет трудно получить доступ к аккаунту без дополнительной информации. Это делает атаки по методу подбора пароля менее эффективными и существенно повышает уровень безопасности.

Дополнительно двухфакторная аутентификация позволяет пользователям контролировать свою безопасность. Многие онлайн-сервисы предоставляют разнообразные методы, такие как SMS-коды, приложения для генерации кодов, а также биометрические данные. Это позволяет пользователям выбирать метод, который наилучшим образом соответствует их предпочтениям и уровню комфорта.

Неоспоримо, что двухфакторная аутентификация содействует усилению безопасности и защите конфиденциальной информации. Ее широкое внедрение и использование становится крайне важным шагом в создании надежных и устойчивых киберзащитных систем.

## 2.2. БИОМЕТРИЧЕСКИЕ МЕТОДЫ. ИХ НАДЕЖНОСТЬ И АЛГОРИТМЫ

Биометрические методы безопасности, основанные на уникальных физиологических и поведенческих характеристиках человека, становятся ключевым элементом в современных системах аутентификации. Эти методы включают в себя использование таких параметров, как отпечатки пальцев, сетчатка глаза, голосовые характеристики и даже образцы фрагментов лица.

Преимущества биометрических методов невозможно переоценить. Во-первых, они основаны на уникальности каждого индивида, что делает подделку или воспроизведение трудным. Во-вторых, биометрические дан-

ные сложно утерять или забыть, в отличие от паролей или ключей. Это снижает риск несанкционированного доступа, связанного с утерей учетных данных.

Процесс работы биометрических методов обычно включает в себя сбор и регистрацию уникальных биометрических данных, их преобразование в шаблон (или хеш) с использованием специализированных алгоритмов и, наконец, сопоставление полученного шаблона с сохраненным в базе данных. Алгоритмы биометрических систем обладают высокой точностью и часто включают в себя сложные математические модели для распознавания и классификации биометрических данных. В качестве примера следует упомянуть про модель машинного обучения BlazeFace, разработанную Google для быстрого определения местоположения и ключевых точек лиц. В модели используются два основных блока для организации архитектуры нейронной сети, представленной на рис. 1. Весь процесс работы технологии можно разделить на 4 этапа: обнаружение, выравнивание, вычисление, валидация. Вычисление параметров состоит из пяти последовательных алгоритмов. Общая структура модели представлена на рис. 2.

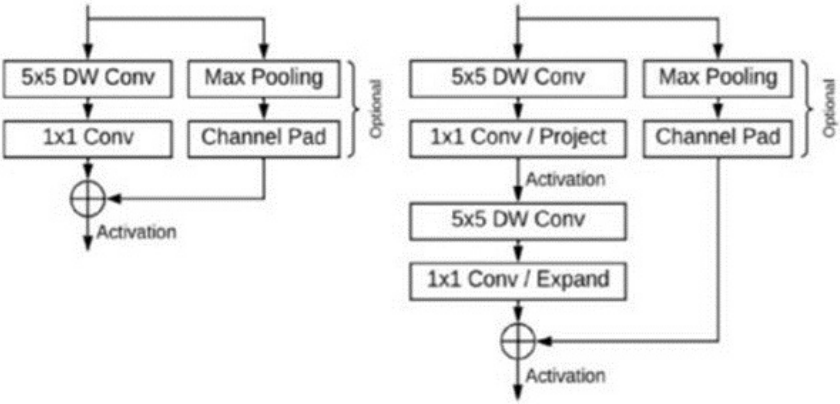


*Рис. 1*. Архитектура нейронной сети

*Fig. 1*. Neural network architecture


*Рис. 2*. Общая структура модели

*Fig. 2.* General structure of the model

Однако, несмотря на все преимущества, биометрические методы не лишены и вызовов. Риск компрометации данных и потенциальные вопросы конфиденциальности становятся актуальными при внедрении таких технологий. Кроме того, возможны ошибки в распознавании, вызванные изменениями в физиологии человека или техническими аспектами работы системы.

В целом, биометрические методы представляют собой сильный и перспективный инструмент в обеспечении безопасности. Их надежность и эффективность продолжают расти с развитием технологий и улучшением алгоритмов, делая их ключевым элементом в современной кибербезопасности.

## 3. АНАЛИЗ ПАРОЛЬНЫХ МЕНЕДЖЕРОВ

### 3.1. ВЗАИМОДЕЙСТВИЕ ПОЛЬЗОВАТЕЛЕЙ С СЕРВЕРАМИ МЕНЕДЖЕРОВ

В современном цифровом мире взаимодействие пользователей с серверами менеджеров осуществляется посредством клиент-серверной модели, которая лежит в основе множества онлайн-сервисов и приложений. Эта модель представляет собой распределенную систему, в которой компьютеры в сети сегментированы на клиентов и серверы.

На стороне клиента находится пользовательское устройство, такое как компьютер, смартфон или планшет. Клиенты инициируют запросы к серверам для получения данных, доступа к ресурсам или выполнения определенных задач. Клиентский компонент обеспечивает визуальный интерфейс и взаимодействует с пользователем, преобразуя его действия в запросы к серверам.

Серверы, в свою очередь, отвечают на запросы клиентов, предоставляя им необходимые ресурсы или данные. Они являются центральными узлами в сетевой инфраструктуре: обрабатывают запросы, управляют базами данных и обеспечивают функциональность, которую клиенты запрашивают.

Клиент-серверная модель взаимодействия, с помощью которой осуществляется обмен информацией между пользователем и сервером, изображена на рис. 3.

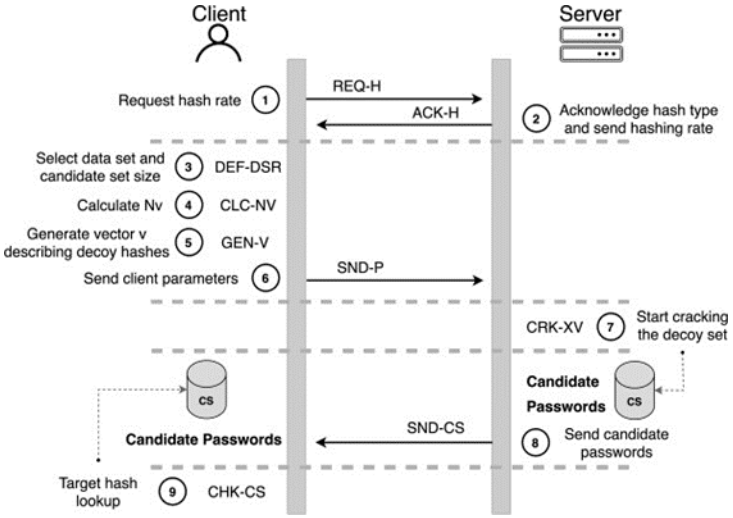


*Рис. 3.* Клиент-серверная модель взаимодействия

*Fig. 3*. Client-server interaction model

Клиент-серверная модель обладает рядом преимуществ. Она обеспечивает масштабируемость, позволяя добавлять новых клиентов и серверы для поддержки роста пользовательской базы. Также она упрощает обновление программного обеспечения, поскольку изменения на сервере могут сразу же отразиться на всех подключенных клиентах. Эта модель является фундаментальной в построении многих современных приложений, включая веб-сервисы, электронную почту, облачные технологии и многое другое.

### 3.2. СРАВНЕНИЕ МЕНЕДЖЕРОВ ПАРОЛЕЙ

В контексте обеспечения безопасности учетных данных сравнение менеджеров паролей становится важным шагом для выбора оптимального решения. Ниже приведены табл. 2 и 3 с ключевыми характеристиками нескольких популярных менеджеров паролей. Знак «минус» означает отсутствие уязвимости, «плюс» – их наличие.

Таблица 2

Table 2

**Сравнение менеджеров на наличие популярных атак**

**Comparison of managers for popular attacks**

| Vulnerabilities | Password Manager | | | |
|---|---|---|---|---|
| | DashLine | LastPass | Keeper | RoboForm |
| Attack. Phishing (app) | - | + | – | – |
| Vulnerabilities: Clipboard (ext) | + | + | + | + |
| Vulnerabilities: PIN Brute Force (app) | + | – | – | + |
| Potential vulnerability: Pwd Brute Force (ext) | + | +– | + | +– |

Уязвимость PIN-кода. Чтобы упростить аутентификацию в приложениях, менеджеры паролей позволяют пользователю установить четырехзначный PIN-код для доступа к приложению. В ходе тестирования было обнаружено, что в RoboForm и DashLine неправильно реализован постоянный счетчик количества раз, когда можно ввести неправильный PIN-код. Было подсчитано, что при атаке методом случайного подбора пароль будет найден за 2,5 часа.

Уязвимость через расширение. Все менеджеры предоставляют расширения для браузера, которые обеспечивают доступ к их хранилищам. Тесты показали, что Keeper, DashLine и 1Password могут быть уязвимы для атаки методом перебора пользовательского интерфейса при вводе главного пароля.

Таблица 3

Table 3

**Сравнение менеджеров на наличие популярных уязвимостей**

**Comparison of managers for popular vulnerabilities**

| Vulnerabilities | Password Manager | | | | |
|---|---|---|---|---|---|
| | DashLine | LastPass | Keeper | 1Password | RoboForm |
| 2FA Speed | – | – | – | – | – |
| Element Inspection | + | + | + | – | – |
| Registration Discovery | + | – | – | – | – |
| URL Mismatch | + | – | + | + | + |
| HTTP(S) Autofill | + | + | + | + | + |
| Ignoring Subdomains | + | + | + | + | + |

2fa Seed. Данная уязвимость была исправлена во всех менеджерах в ходе обновления ПО.

Element Inspection представляет собой утечку общих паролей через инструменты проверки элементов DOM, таких как Chrome. Тестирование выявило, что предоставление ограниченного доступа к паролю другому пользователю после входа в систему под другими данными открывает пароль. Только менеджеры 1Password и RoboForm не имеют данной уязвимости.

Registration Discovery Vulnerability. Данная уязвимость срабатывает, если попытаться войти в систему с неверным логином, а затем с неверным паролем. Уязвимость была найдена только у DashLine.

URL Mismatch. Данная уязвимость означает то, что поля входа в систему заполняются именем пользователя и паролем, несмотря на то что URL-адреса источника и назначения не совпадают. Данный бэкдор существует у всех рассматриваемых менеджеров, кроме LastPass.

HTTP(S) Autofill. Политики автозаполнения не различают HTTP и HTTPS при попытке заполнить учетные данные. Это позволяет злоумышленнику выдать себя за HTTP-версию популярного сайта и украсть учетные данные пользователя, изначально сохраненные для версии HTTPS. Данная уязвимость есть во всех тестируемых менеджерах.

Ignoring Subdomains. Субдомены игнорируются при заполнении паролей. Таким образом, злоумышленник в субдомене может украсть учетные данные пользователя для родительского домена или других субдоменов. Данная проблема касается всех пяти менеджеров паролей.

Исходя из полученных результатов исследований можно сделать вывод, что, несмотря на широкий спектр функциональности, необходимо уделять особое внимание вопросам безопасности. Осведомленность о возможных уязвимостях является ключевым элементом в обеспечении надежной защиты пользовательских паролей и конфиденциальной информации.

## ЗАКЛЮЧЕНИЕ

Современные методы хранения паролей представляют собой важную составляющую безопасности информации. Существует множество способов защиты паролей от несанкционированного доступа – от использования хэширования и солей до двухфакторной аутентификации. Однако, несмотря на все усилия, важно помнить, что ни один метод хранения паролей не является абсолютно непроницаемым. Поэтому важно не только использовать современные методы хранения паролей, но и следить за их обновлением и регулярно менять пароли для обеспечения максимальной безопасности.

## СПИСОК ЛИТЕРАТУРЫ

1. Synopsys Inc. Sentaurus’ Device User Guide: Version M-2016.12. – December 2016.

2. *Петросянц К.О.* Состояние работ в области моделирования полупроводниковых компонентов с учетом влияния радиации и температуры // Наноиндустрия. – 2018. – № 82. – С. 42–45.

3. *Dorckel J.M., Leturcq P.H.* Carrier mobilities in silicon semi-empiriccally related to temperature, doping and injection level // Solid-State Electronis. – 1981. – Vol. 24 (9). – P. 821–825.

4. *Резевиг В.Д.* Применение программ P-CAD и PSpice для схемотехнического моделирования на ПЭВМ. Вып. 2. Модели компонентов аналоговых устройств. – М.: Радио и связь, 1992. – 64 с.

5. *Green M.A.* Intrinsic concentration, effective density of states, and effective mass in silicon // Journal of Applied Physics. – 1990. – Vol. 67. – P. 2944–2954.

6. *Черкесова Ж.Ж., Карданов З.С.* Методы хранения паролей // Аллея науки. – 2017. – Т. 2, № 16. – С. 457–460.

7. *Костеров В.Б.* Методы хранения паролей в базах данных // Мавлютовские чтения: материалы XVI Всероссийской молодежной научной конференции. В 6 т. Т. 5. – Уфа, 2022. – С. 605–609.

8. *Арзиева Ж.Т., Арзиев А.Т.* Анализ методов генерации одноразовых паролей и высокая степень случайности генерируемых паролей // Бюллетень науки и практики. – 2022. – Т. 8, № 7. – С. 382–388. – DOI: 10.33619/2414-2948/80/35.

9. *Галатенко В.А.* Основы информационной безопасности: курс лекций. – М.: ИНТУИТ, 2016. – 129 с.

10. Исследование системы идентификации и подтверждения легитимности доступа на основе динамических методов биометрической аутентификации / М.М. Путято, А.С. Макарян, Ш.М. Чич, В.К. Маркова // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3 (51). – С. 83–93. – DOI: 10.21672/2074-1707.2020.51.1.083-093.

11. *Jayavadivel R., Prabaharan P.* Investigation on automated surveillance monitoring for human identification and recognition using face and iris biometric // Journal of Ambient Intelligence and Humanized Computing. – 2021. – Vol. 12 (11). – P. 10197–10208. DOI: 10.1007/s12652-020-02787-1.

12. *Tiong L.C.O., Kim S.T., Ro Y.M.* Implementation of multimodal biometric recognition via multi-feature deep learning networks and feature fusion // Multimedia Tools and Applications. – 2019. – Vol. 78 (22). – P. 22743–22772. – DOI: 10.1007/s11042-019-7618-0.

13. An evaluation of denoising techniques and classification of biometric images based on deep learning / S. Arora, R. Mittal, H. Kukreja, M.P.S. Bhatia // Multimedia Tools and Applications. – 2022. – Vol. 82 (6). – P. 8287–8302. – DOI: 10.1007/s11042-021-11573-w.

14. *Павлоцкий И.П., Косов Н.А.* Обзор известных проблем и угроз безопасности менеджеров паролей // Вопросы устойчивого развития общества. – 2021. – № 6. – С. 569–574.

15. *Каримов М.М., Арзиева Ж.Т., Худойкулов З.Т.* Выбор соответствующих генераторов псевдослучайных чисел для генераторов одноразовых паролей // Наука в современном мире: материалы Международной (заочной) научно-практической конференции, Душанбе, 23 июля 2019 г. – Душанбе, 2019. – С. 21–30.

16. *Knuth D.E.* Art of computer programming. Vol. 2. Seminumerical algorithms. – Addison-Wesley Professional, 2014.

17. *Jagannatam A.* Mersenne Twister – a pseudo random number generator and its variants. – George Mason University, Department of Electrical and Computer Engineering, 2008.

18. American national standard for financial institution key management. Technical Report ANSI X.917. – American Bankers Association, 1985.

19. Security analysis of pseudo-random number generators with input:/dev/random is not robust / Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergniaud, D. Wichs // Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13). – ACM, 2013. – P. 647–658. – DOI: 10.1145/2508859.2516653.

20. *Dorrendorf L., Gutterman Z., Pinkas B.* Cryptanalysis of the random number generator of the Windows operating system // ACM Transactions on Information and System Security. – 2009. – Vol. 13 (1). – Art. 10. – DOI: 10.1145/1609956.1609966.

***Рябцев Денис Константинович***, лаборант кафедры защиты информации Новосибирского государственного технического университета. E-mail: ryabtsev@mail.ru

DOI: 10.17212/2782-2230-2024-1-74-89

## Analysis of modern password storage methods*

**D.K. Ryabtsev**

*Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Security Department. E-mail: ryabstev@mail.ru*

The article "Analysis of modern password storage methods" provides comprehensive a comprehensive review of existing approaches to secure password storage in modern information systems. The study covers technologies used to protect credentials and their effectiveness in the context of growing cybersecurity threats.
The reader will gain a deep understanding of the advantages and disadvantages of various password storage methods, as well as recommendations for choosing the most reliable and modern solutions.

**Keywords**: password security, hashing, salt in password protection, cryptography, multifactor authentication, biometric technologies

* *Received 15 February 2024.*

**REFERENCES**

1. Synopsys Inc. Sentaurus Device User Guide, Version M-2016.12. December 2016.

2. Petrosyants K.O. Sostoyanie rabot v oblasti modelirovaniya poluprovodnikovykh komponentov s uchetom vliyaniya radiatsii i temperatury [The status of semiconductor components modeling with respect to thermal and radiation effects]. Nanoindustriya = Nanoindustry, 2018, no. 82, pp. 42–45.

3. Dorckel J.M., Leturcq P.H. Carrier mobilities in silicon semi-empiriccally related to temperature, doping and injection level. Solid-State Electronis, 1981, vol. 24 (9), pp. 821–825.

4. Rezevig V.D. Primenenie programm P-CAD i PSpice dlya skhemotekhnicheskogo modelirovaniya na PEVM. Vyp. 2. Modeli komponentov analogovykh ustroistv [Application of P-CAD and PSpice programs for schematic modeling on PC. Iss. 2. Models of analogue devices components]. Moscow, Radio i svyaz' Publ., 1992. 64 p.

5. Green M.A. Intrinsic concentration, effective density of states, and effective mass in silicon. Journal of Applied Physics, 1990, vol. 67, pp. 2944–2954.

6. Cherkesova Zh.Zh., Kardanov Z.S. Metody khraneniya parolei [Methods of storing passwords]. Alleya nauki, 2017, vol. 2, no. 16, pp. 457–460. (In Russian).

7. Kosterov V.B. [Methods of storing passwords in databases]. Mavlyutovskie chteniya [Mavlyutov readings]. Materials of the XVI All-Russian Youth Scientific Conference. In 6 vols. Vol. 5. Ufa, 2022, pp. 605–609. (In Russian).

8. Arzieva Zh.T., Arziev A.T. Analiz metodov generatsii odnorazovykh parolei i vysokaya stepen' sluchainosti generiruemykh parolei [Analysis of methods for generating one-time passwords and a high degree of randomness of generated passwords]. Byulleten' nauki i praktiki = Bulletin of Science and Practice, 2022, vol. 8, no. 7, pp. 382–388. DOI: 10.33619/2414-2948/80/35.

9. Galatenko V.A. Galatenko V.A. Osnovy informatsionnoi bezopasnosti [Fundamentals of information security]. Moscow, Internet University of Information Technologies (INTUIT) Publ., 2016. 129 p.

10. Putyato M.M., Makaryan A.S., Chich Sh.M., Markova V.K. Issledovanie sistemy identifikatsii i podtverzhdeniya legitimnosti dostupa na osnove dinamicheskikh metodov biometricheskoi autentifikatsii [System development for identification and confirmation of access legitimacy based on biometric authentication dynamic methods]. Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies, 2020, no. 3 (51), pp. 83–93. DOI: 10.21672/2074-1707.2020.51.1.083-093.

11. Jayavadivel R., Prabaharan P. Investigation on automated surveillance monitoring for human identification and recognition using face and iris biometric.

Journal of Ambient Intelligence and Humanized Computing, 2021, vol. 12 (11), pp. 10197–10208. DOI: 10.1007/s12652-020-02787-1.

12. Tiong L.C.O., Kim S.T., Ro Y.M. Implementation of multimodal biometric recognition via multi-feature deep learning networks and feature fusion. Multimedia Tools and Applications, 2019, vol. 78 (22), pp. 22743–22772. DOI: 10.1007/s11042-019-7618-0.

13. Arora S., Mittal R., Kukreja H., Bhatia M.P.S. An evaluation of denoising techniques and classification of biometric images based on deep learning. Multimedia Tools and Applications, 2022, vol. 82 (6), pp. 8287-8302. DOI: 10.1007/s11042-021-11573-w.

14. Pavlotskii I.P., Kosov N.A. Obzor izvestnykh problem i ugroz bezopasnosti menedzherov parolei [Overview of known password manager security issues and threats]. Voprosy ustoichivogo razvitiya obshchestva, 2021, no. 6, pp. 569–574. (In Russian).

15. Karimov M.M., Arzieva Zh.T., Khudoikulov Z.T. [The choice of appropriate pseudorandom number generators for one-time password generators]. Nauka v sovremennom mire [Science in the modern world]. Materials of an International (correspondence) Scientific and Practical Conference, Dushanbe, July 23, 2019, pp. 21–30. (In Russian).

16. Knuth D.E. Art of computer programming. Vol. 2. Seminumerical algorithms. Addison-Wesley Professional, 2014.

17. Jagannatam A. Mersenne Twister – a pseudo random number generator and its variants. George Mason University, Department of Electrical and Computer Engineering, 2008.

18. American national standard for financial institution key management. Technical Report ANSI X.917. American Bankers Association, 1985.

19. Dodis Y., Pointcheval D., Ruhault S., Vergniaud D., Wichs D. Security analysis of pseudo-random number generators with input: /dev/random is not robust. Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13). ACM, 2013, pp. 647–658. DOI: 10.1145/2508859.2516653.

20. Dorrendorf L., Gutterman Z., Pinkas B. Cryptanalysis of the random number generator of the Windows operating system. ACM Transactions on Information and System Security, 2009, vol. 13 (1), art. 10. DOI: 10.1145/1609956.1609966.

Для цитирования:

*Рябцев Д.К.* Анализ современных методов хранения паролей // Безопасность цифровых технологий. – 2024. – № 1 (112). – С. 74–89. – DOI: 10.17212/2782-2230-2024-1-74-89.

For citation:

Ryabtsev D.K. Analiz sovremennykh metodov khraneniya parolei [Analysis of modern password storage methods]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 1 (112), pp. 74–89. DOI: 10.17212/2782-2230-2024-1-74-89.